Remarks

Status of application

Claims 1-58 were examined and stand rejected in view of prior art. The claims have been amended to further clarify Applicant's invention. Reexamination and reconsideration are respectfully requested.

The invention

A security system with methodology for defending against security breaches of peripheral devices is described. In one embodiment, for example, a method of the present invention includes protecting a computer from security breaches involving devices that may be attached to the computer, the method comprises steps of: when a device is first attached to the computer, requiring user-provided information for authorizing the device; based on the user-provided information, storing authorization information indicating whether or not that the device is allowed to communicate with the computer; detecting detachment of the device from the computer; updating the authorization information to indicate that the device is no longer authorized to communicate with the computer; and upon reattachment of the device, blocking communication with the device while the device remains unauthorized, thereby preventing a security breach involving the device.

General

Certain editing informalities in the claims were observed and have been corrected.

Prior art rejections

A. Section 102(e) rejection: Heinrich

Claims 1-58 stand rejected under U.S.C. 102(e) as being anticipated by Heinrich et al. (Pub. No. 2002/0194486) ("Heinrich"). Here, the Examiner likens Applicant's invention to a security system for securing certain Plug and Play peripheral devices connected to an ISA (i.e., PC internal) bus. The Examiner's rejection of claims 1, 23, and 43 is representative:

> Regarding claims 1, 23 and 43, Heinrich discloses when a device is first attached to the computer, specifying authorization information indicating that the device is allowed to communicate with the computer (Heinrich: paragraphs [0009, 0021]); detecting detachment of the device from the computer (Heinrich: see Abstract section); updating the authorization information to indicate that the device is no longer authorized to communicate with the computer (Heinrich: paragraphs [0016-0017 and 0045]); and upon reattachment of the device, blocking communication with the device while the device remains unauthorized, thereby preventing a security breach involving the device (Heinrich: paragraphs [0009, 0015 and 0034-0035], the device remains locked until the passwords match).

Applicant's claims have been amended to prevent the interpretation that they read on Heinrich.

Heinrich describes a security system for Plug and Play peripheral devices that is internal to the computer system (i.e., it does not involve the user in the process), especially when used in the context of connecting devices to an ISA bus (e.g., inserting a video card into the internal bus slot on a PC). Of particular interest to Heinrich is that those peripheral devices may contain sensitive information or passwords. Therefore, Heinrich approach is to protect those peripheral devices from security breaches (i.e., coming from the computer).

Heinrich is essentially the opposite scenario that is addressed by Applicant's invention. The problem addressed by Applicant's invention is that "bad" (untrustworthy) devices may be plugged into a computer. A "bad" peripheral device for example would include a keyboard having an in-line (e.g., dongle) key logger. In that case, the keyboard is untrustworthy (since it may steal user-provided information) and, therefore, it should be blocked (i.e., denied access) from communicating with the computer. In Heinrich's scenario, on the other hand, the peripheral devices themselves are secured (i.e., they contain sensitive information, and thus are required to be secured against unauthorized access). In that scenario, the peripheral devices themselves are not bad, but instead they

are "good" devices having valuable information that should be protected from unauthorized access.

Recognizing that (when broadly interpreted) Applicant's claims could be construed to read on Heinrich's fundamentally different system, Applicant's independent claims were amended to highlight the above-mentioned distinctions. An important distinction is that Applicant's approach requires the user to authorize the particular peripheral device (being attached). Here, user inspection is desirable to determine if a peripheral device has been tampered with. In Heinrich's approach, on the other hand, an internal hardware system operates to keep track of identifying information of various Plug and Play devices inserted and reinserted into slots connected to the ISA bus (i.e., internal computer bus); there is no user interaction. Essentially, Heinrich is a housekeeping or accounting approach to track the movement of known "good" peripheral devices and cards (e.g., when moved from one slot to another). Importantly, Heinrich includes no provision where his system prompts for user authorization before a device is accepted as trusted. In other words, if someone decided to plug a "bad" card into Heinrich's system (e.g., one that has been physically tampered with), Heinrich has no mechanism to prompt the user to check out the newly-attached or plugged-in device to see if it is legit.

Applicant's independent claims have been amended to bring these distinctions to the forefront. For example, claim 1 includes the claim limitation:

> when a device is first attached to the computer, requiring user-provided information for authorizing the device;

Here, the claim makes it clear that Applicant's claimed approach basically assumes any attached device is un-trusted until proven otherwise. A device becomes trusted once a user (with appropriate privileges) indicates that he or she is vouching for the device (e.g., by entering information indicating that the device is authorized for attachment to the computer, for example after appropriate visual inspection of the device). The user himself or herself may be located at the machine, or may be located remotely (e.g., remote administrator). If the device is not authorized by the user, then the device retains

its un-trusted status, whereupon communication of the un-trusted device with the computer is blocked. For example in the case of a "bad" keyboard, the keyboard would be blocked from communicating with the computer (i.e., it would not work). Importantly in this scenario, when a trusted device becomes unplugged and then is later reattached, Applicant's approach is to treat it as an un-trusted device again (until such time that it can be re-authenticated by the user).

In view of the foregoing and amendments to the independent claims, it is respectfully submitted that Applicant's invention provides an important and patentable advance over the art. Using Applicant's invention, for example, it is now possible to detect malicious tampering of peripheral devices. For example, if a bad guy attempted to unplug a keyboard at a public Internet café for purposes of inserting a key logger dongle, Applicant's invention would catch that event and would refuse to reauthorize the keyboard (as the bad guy would not have sufficient rights to enter a password authorizing the keyboard), until such time as an appropriately authorized individual (e.g., Internet café employee) came along, inspected the keyboard for tampering, and then reauthorized the keyboard (if observed to be untampered). Applying the teachings of Heinrich to this scenario would not work. Heinrich simply has no mechanism described that detects attempts to tamper peripheral devices, and certainly has no mechanism where it refuses the reattachment of peripheral devices that are not authorized by the user. Accordingly, the amended claims are believed to distinguish over the cited art, and any rejection under Section 102 is overcome.

Any dependent claims not explicitly discussed are believed to be allowable by virtue of dependency from Applicant's independent claims, as discussed in detail above.

Conclusion

In view of the foregoing remarks and the amendment to the claims, it is believed that all claims are now in condition for allowance. Hence, it is respectfully requested that the application be passed to issue at an early date.

If for any reason the Examiner feels that a telephone conference would in any way expedite prosecution of the subject application, the Examiner is invited to telephone the

undersigned at 408 884 1507.

Respectfully submitted,

Date: July 24, 2007

/John A. Smart/

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
815 572 8299 FAX